



**OAS Meetings of the Ministers of Justice or Attorneys General of the Americas  
9th Meeting of the Working Group on Cybercrime, 12-13 Dec 2016, Washington DC  
Agenda item “International legal frameworks”**

# **Implementation of the Budapest Convention on Cybercrime**

**Alexander.seger@coe.int**



**[www.coe.int/cybercrime](http://www.coe.int/cybercrime)**

# COE approach on cybercrime

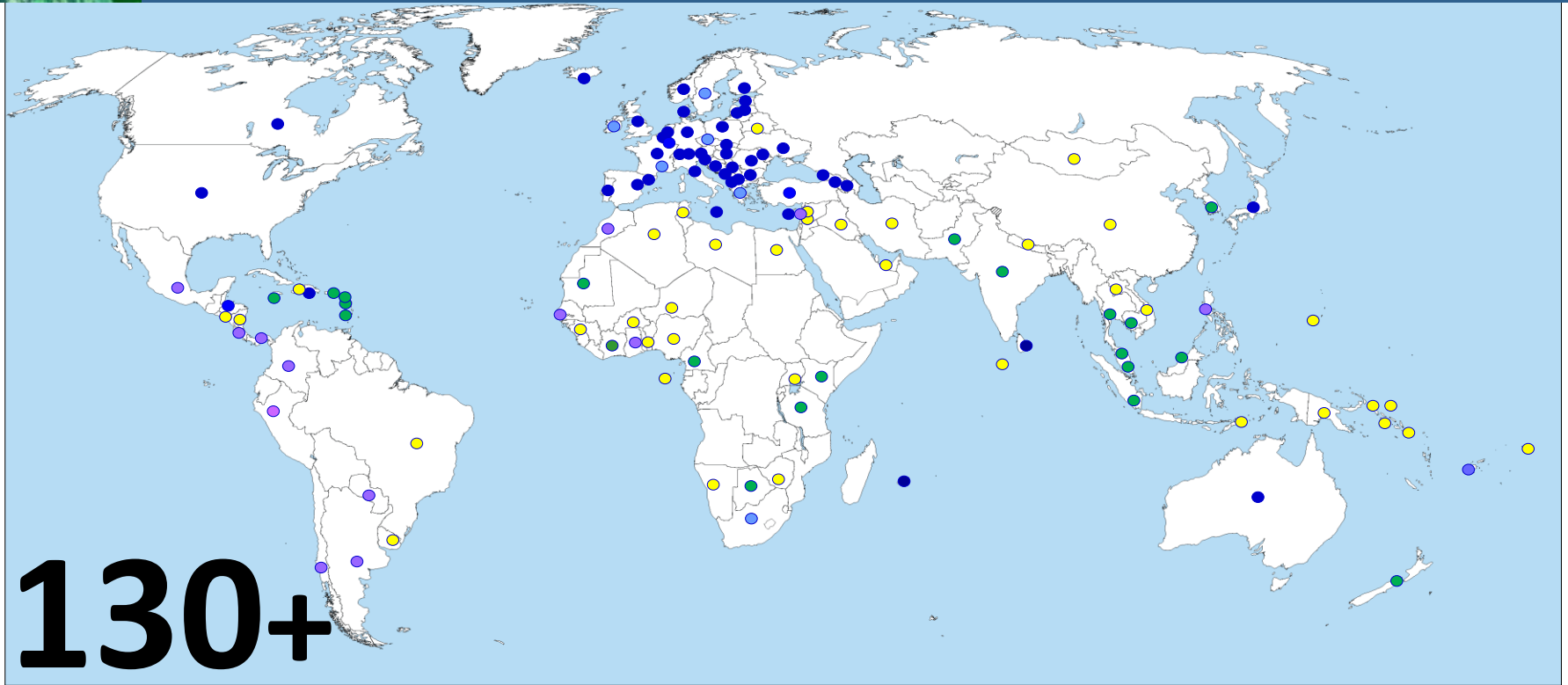
**1 Common standards: Budapest Convention on Cybercrime and relates standards**

**2 Follow up and assessments:  
Cybercrime  
Convention  
Committee (T-CY)**



**3 Capacity building:  
C-PROC ►  
Technical cooperation  
programmes**

# Reach of the Budapest Convention as a guideline

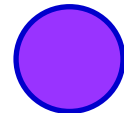
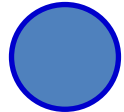
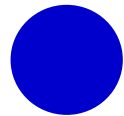


Indicative map only

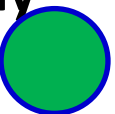
**Budapest Convention  
Ratified/acceded: 50**

**Signed: 5**

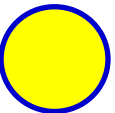
**Invited to accede: 12  
= 67**



**Other States with laws/draft laws largely  
in line with Budapest Convention = 20**



**Further States drawing on Budapest  
Convention for legislation = 45+**





# OAS Member States and the Budapest Convention

## **Parties:**

- **Canada**
- **Dominican Republic**
- **Panama**
- **USA**

## **Invited to accede:**

- **Argentina**
- **Chile**
- **Colombia**
- **Costa Rica**
- **Mexico**
- **Paraguay**
- **Peru**

# Contents of the Budapest Convention

## Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

## Procedural tools

- Expedited preservation
- Search and seizure
- Interception of computer data

+

## International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation



# Cybercrime Convention Committee (T-CY)

## Established under Article 46 Budapest Convention

### **Membership**

**(status December 2016):**

- **50 Members (State Parties)**
- **17 Observer States**
- **10 International organisations (African Union Commission, Commonwealth Sec, ENISA, European Union, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)**

### **Functions:**

- **Assessments of the implementation of the Convention by the Parties**
- **Guidance Notes**
- **Draft legal instruments**
- **Etc.**

**2 x plenaries per year  
+ Bureau and Working Group meetings**



# T-CY Guidance Notes

## **Guidance Notes adopted:**

- ✓ **Notion of “Computer Systems”**
- ✓ **Botnets**
- ✓ **Identity theft**
- ✓ **DDOS attacks**
- ✓ **Critical Infrastructure Attacks**
- ✓ **Malware**
- ✓ **Transborder access to data (Article 32)**
- ✓ **Terrorism**

## **Guidance Note under negotiation:**

- **Production order for subscriber information (Article 18)**



# Crime and jurisdiction in cyberspace ► solutions proposed under the Budapest Convention on Cybercrime

## Context:

Budapest Convention on Cybercrime ► Cybercrime Convention Committee (T-CY) ► Cloud Evidence Group ► Recommendations September 2016 ► now under consideration by T-CY

## Rationale:

- Cybercrime AND electronic evidence in relation to any crime
- E-evidence on servers in foreign, unknown, multiple or shifting jurisdictions, in the cloud
- No data, no evidence, no prosecution, no justice, no rule of law (in cyberspace)

## Issues:

- Differentiating subscriber versus traffic versus content data
- Limited effectiveness of MLA
- Loss of location and transborder access jungle
- Provider present or offering a service in the territory of a Party
- Voluntary disclosure by US-providers
- Emergency procedures
- Data protection

## Solutions:

1. More efficient MLA
2. Guidance Note on Article 18
3. Domestic rules on production orders (Article 18)
4. Cooperation with providers: practical measures
5. Protocol to Budapest Convention



# CAPACITY BUILDING ON CYBERCRIME

Council of Europe projects underway

**Cybercrime@Octopus** (voluntary contribution funded)



**GLACY+** EU/COE Joint Project on Global Action on Cybercrime Extended

**Cybercrime@EAP II** (International cooperation) in Eastern Partnership countries

**Cybercrime@EAP III** (public/private cooperation)

**iPROCEEDS** EU/COE Joint Project targeting proceeds from crime online in South-eastern Europe

Managed by:

**C-PROC** Cybercrime Programme Office of the Council of Europe  
(Bucharest, Romania)



# Conclusions

- ▶ **States invited to accede (Chile, Colombia, Costa Rica, Mexico, Paraguay and Peru) to accelerate process and complete accession.**
- ▶ **GLACY+ Project as an opportunity.**
- ▶ **Other States to consider accession.**
- ▶ **Council of Europe available to review/support domestic legislation.**
- ▶ **COE/OAS to cooperate when supporting States.**